UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ROBIN STEVEN, SEAN MUNGIN and DEVONNE MCMORRIS on behalf of themselves, all others similarly situated, and the general public, Plaintiffs, v. CARLOS LOPEZ & ASSOCIATES, LLC, CARLOS LOPEZ, individually, Defendants.	Case No.: 18-cv-6500 CLASS ACTION **FIRST AMENDED COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs ROBIN STEVEN, SEAN MUNGIN and DEVONNE MCMORRIS (hereinafter referred to as "Plaintiffs"), on behalf of themselves, all others similarly situated, and the general public, by and through their undersigned counsel, Derek Smith Law Group, PLLC, hereby bring this action against CARLOS LOPEZ & ASSOCIATES, LLC and CARLOS LOPEZ, individually, (hereinafter referred to as "CLA"), and allege the following upon their own knowledge, or where they lack personal knowledge, upon information and belief including the investigation of their counsel.

INTRODUCTION

1. Defendant, Carlos Lopez and Associates, LLC, is a mental and behavioral health service provider, comprised of professionals and para-professionals providing mental health services to veterans, service members, family member and community members generally.

2. Defendant, Carlos Lopez and Associates, LLC employs approximately 100 employees and maintains the personal information of each employee, including social security

numbers, current home addresses, dates of birth, telephone numbers, educational degree, dates of hire and other identifying information of employees.

3. On more than one occasion, the Human Resources Department of CLA, and specifically Defendant CLA's employee Rosemary Torres, failed to safeguard sensitive information and sent sensitive information to employees who were not supposed to be privy to the information.

4. Employees whose information had been improperly shared complained to senior management about these negligent acts of the Human Resources Department of CLA, and Defendant CLA's employee Rosemary Torres, but Defendant CLA failed to take any corrective action.

5. Around June 29, 2018, Defendant CLA's employee Rosemary Torres sent an email with a spreadsheet attachment to the email addresses of the entire CLA company. The spreadsheet attachment contained the personal information of each current and former employee of Defendant CLA, totaling approximately 130 individuals, including social security numbers, current home addresses, dates of birth, telephone numbers, educational degree, dates of hire and other identifying information of employees.

6. Defendant breached its duty to protect and safeguard Plaintiffs and Class Members' personal information and to take reasonable steps to contain the damage caused where such information was compromised. Through no fault of their own, Plaintiffs and Class Members have suffered financial and emotional injury and must now attempt to safeguard themselves and their families from unknown but certainly impending future crimes. For the reasons set forth below, Plaintiffs and Class Members request damages to compensate them for current and future losses, as well as injunctive relief to provide safeguards against

another failure of Defendant's personal information storage systems and processes. In addition, Plaintiffs and Class Members seek credit monitoring services uniquely tailored to protect the interests of the victims of this data breach, to monitor their credit and proactively guard against future identity theft and fraud.

7. Accordingly, Plaintiffs bring this class action to remedy violations of common law claims for negligence, negligence per se, as well as statutory claims under state consumer protection statutes, on behalf of separate statewide classes for the states of California, Florida, Texas, Maine, New Jersey and New York, as described below.

INTRADISTRICT ASSIGNMENT

8. Pursuant to Local Civil Rule 50.1(d)(2)(b)(1), this action is properly assigned to the Manhattan Courthouse, because, as further set forth herein, a substantial part of the events or omissions giving rise to the claims occurred in New York County.

THE PARTIES

9. Plaintiff ROBIN STEVEN is a resident of New York, Bronx County, and was previously employed by Defendant CLA.

10. Plaintiff SEAN MUNGIN is a resident of California, Los Angeles County, and was previously employed by Defendant CLA.

11. Plaintiff DEVONNE MCMORRIS is a resident of New York, Westchester County, and is currently employed by Defendant CLA.

12. Defendant CARLOS LOPEZ & ASSOCIATES, LLC, is a Texas Limited Liability Company with its principal place of business in Lincoln Maine.

13. Defendant CARLOS LOPEZ, is a resident of the sate of Maine, Penobscot County.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), the Class Action Fairness Act, because the matter in controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs, at least one member of the class of Plaintiffs is a citizen of a State different from Defendant CLA. In addition, more than two-thirds of the members of the class reside in states other than the state in which Defendant is a citizen and less than one-third of the members of the class reside in states other than the state in which this case is filed. Therefore any exceptions to jurisdiction under 28 U.S.C. § 1332(d) do not apply.

15. The Court has personal jurisdiction over Defendant CLA, because Defendant regularly conducts business in New York. Furthermore, Defendant advertised, marketed, distributed, offered for sale, and sold its services to consumers in New York and the United States, transacting business in New York County, in New York, and throughout the United States, including without limitation online marketing intended to reach consumers in New York County. Moreover, Defendant CLA has sufficient purposeful, systematic, and continuous minimum contacts with the various states of the United States, including New York, and has sufficiently availed itself of the markets of various states of the United States, including New York, to render the exercise of personal jurisdiction by this Court permissible.

16. Venue is proper in the Southern District of New York pursuant to 28 U.S.C. § 1391(b) and (c), because a substantial portion of the acts forming the basis for the claims

occurred in this district, and because Defendant CLA transacts substantial business generally in this district.

FACTS

17. Defendant, Carlos Lopez and Associates, LLC, is a mental and behavioral health service provider, comprised of approximately 100 professionals and para-professionals providing mental health services to veterans, service members, family member and community members generally.

18. As a condition of employment, Defendant CLA requires employees to provide personal identifying information ("PII") as a condition of employment, and Defendant CLA maintains the personal information of each employee, including social security numbers, current home addresses, dates of birth, telephone numbers, educational degree, dates of hire and other identifying information of employees.

19. On more than one occasion, the Human Resources Department of CLA, and specifically Defendant CLA's employee Rosemary Torres, failed to safeguard sensitive information and sent sensitive information to employees who were not supposed to be privy to the information. Employees whose information had been improperly shared complained to senior management about these negligent acts of the Human Resources Department of CLA, and Defendant CLA's employee Rosemary Torres, but Defendant CLA failed to take any corrective action.

20. Around June 29, 2018, Defendant CLA's employee Rosemary Torres sent an email with a spreadsheet attachment to the email addresses of the entire company. The spreadsheet attached contained the personal information of each current and former employee

of Defendant CLA, totaling approximately 130 individuals, including social security numbers, current home addresses, dates of birth, telephone numbers, educational degree, dates of hire and other identifying information of employees.

21. The PII of Plaintiff ROBIN STEVEN, a former employee of Defendant CLA, was on the spreadsheet attached to the email sent to the entire CLA company.

22. The PII of Plaintiff SEAN MUNGIN, a former employee of Defendant CLA, was on the spreadsheet attached to the email sent to the entire CLA company.

23. The PII of Plaintiff DEVONNE MCMORRIS, a current employee of Defendant CLA, was on the spreadsheet attached to the email sent to the entire CLA company.

24. Defendant waited until July 13, 2018, two weeks after the data breach, to send an email to the employees of CLA addressing the breach, and failed to take any proper corrective action.

25. To date, Defendant CLA has failed to contact the former employees of the company, including Plaintiffs, to address the breach.

26. Defendant CLA did not offer to provide employees or former employees with any safeguard of monitoring to prevent the data breach from resulting in identity theft of fraud.

27. Defendant breached its duty to protect and safeguard the Plaintiffs' and Class Members' personal information and to take reasonable steps to contain the damage caused where such information was compromised.

28. Through no fault of their own, Class Members have suffered financial and emotional injury and must now attempt to safeguard themselves and their families from unknown but certainly impending future crimes.

29. For the reasons set forth below, Plaintiffs and Class Members request damages to compensate them for current and future losses, as well as injunctive relief to provide safeguards against another data breach of Defendant's PII systems. In addition, Plaintiffs and Class Members seek credit monitoring services uniquely tailored to protect the interests of the victims of this data breach, to monitor their credit and proactively guard against future identity theft and fraud.

30. Accordingly, Plaintiffs bring this class action to remedy violations of common law claims for negligence, negligence per se, as well as statutory claims under state consumer protection statutes, on behalf of separate statewide classes for the states of California, Florida, Texas, Maine, New Jersey and New York, as described below.

31. Defendant CLA owed a common law duty to the Plaintiffs and Class Members, who entrusted Defendant with sensitive Personal Information, to exercise reasonable care in receiving, maintaining and storing Personal Information in Defendant's possession. Defendant owed a duty to prevent Class Members' Personal Information from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. Part and parcel of Defendant's duty was the obligation to provide reasonable security consistent with industry best practices and requirements, and to ensure Information Technology systems and networks, and the personnel responsible for those systems and networks adequately protected Class Members' Personal Information.

32. Defendant owed a duty to Plaintiffs and Class Members, who entrusted Defendant with sensitive Personal Information, to design, maintain, and test the Information Technology systems that housed Class Members' Personal Information, and to ensure that the Personal Information in Defendant's possession was adequately secured and protected.

33. Defendant owed a duty to Plaintiffs and Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the Personal Information stored in Defendant's computer systems. This duty required Defendant to adequately train employees and others with access to Class Members' Personal Information on the procedures and practices necessary to safeguard sensitive Personal Information.

34. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would enable Defendant to timely detect a breach of its Information Technology systems.

35. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings such as the employee reports of misuse and misappropriation of sensitive personal information of employees by Defendant CLA's Human Resources Department in a timely fashion.

36. Defendant owed a duty to Plaintiffs and Class Members to disclose when and if Defendant's Information Technology systems and data security practices were not sufficiently adequate to protect and safeguard Class Members' Personal Information.

37. Defendant owed a duty to Plaintiffs and Class Members to timely disclose the fact that a data breach had occurred.

38. Defendant owed these duties to Plaintiffs and Class Members because Plaintiffs and Class Members were foreseeable and probable victims of Defendant's inadequate data security practices. Accordingly, Defendant CLA knew or should have known that a breach of its PII systems would cause Plaintiffs and Class Members to incur damages and suffer harm as described herein.

39. Victims of the Defendant's data breach are at imminent risk of suffering identity theft.

40. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[1] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[2]

41. Social security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

42. The Social Security Administration has warned that identity thieves can use an individual's social security number and good credit score to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[3]

43. Stolen social security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her social security number was used to file for unemployment benefits until law

[1] 17 C.F.R. § 248.201 (2013).
[2] *Id.*
[3] Social Security Administration, Identity Theft and Your Social Security Number, *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 16, 2018).

enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

44. What is more, it is no easy task to change or cancel a stolen social security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse is not typically permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

45. Even then, a new social security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[4]

46. Another danger, according to the publisher of *Privacy Journal*, Robert Ellis Smith, is that cyber attackers use stolen social security numbers to obtain medical care in someone else's name.[5] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[6] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[7] Further, a report released by the Ponemon Institute concluded that 65 percent of medical identity theft victims

[4] Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data- stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited July 16, 2018).
[5] *Id.*
[6] CNET, *Study: Medical identity theft is costly for victims*, http://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited July 16, 2018).
[7] *Id.*

spend 200 hours with insurers and providers to secure their credentials and check the accuracy of their personal information, invoices, and e-health records.[8]

47. Based on the foregoing, the information compromised in the CLA data breach is significantly more valuable to those with access to the information than, say, credit card information obtained in a large retailer data breach. Victims affected by retailer breaches could avoid much of the potential for future harm by cancelling credit or debit cards and obtaining replacements. The information compromised in the CLA breach is difficult, if not impossible, to change—social security number, name, date of birth, employment information, etc.

48. This data, as one would expect, commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, has explained that on the black market, PII and social security numbers are worth ten times the price of stolen credit card information.[9]

49. Additionally, credit-monitoring services, while helpful, are insufficient. Noted cybersecurity journalist, and blogger Brian Krebs has explained: "[T]he sad truth is that most services offer little in the way of real preventative protection against the fastest-growing crime in America [identity theft]."[10] Credit monitoring services, in other words, may inform individuals of fraud after the fact, but do little to thwart fraud from occurring in the first instance.

---

[8] Ponemon Institute, 2014 Fifth Annual Study on Medical Identity Theft, *available at* https://www.ponemon.org/local/upload/file/2013%20Medical%20Identity%20Theft%20Report%20FINAL%2011.pdf (last visited July 16, 2018).

[9] Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, Tim Greene, Feb. 6, 2015, *available* https://www.networkworld.com/article/2880366/security0/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 16, 2018).

[10] Brian Krebs, Are Credit Monitoring Services Worth It?, Krebs on Security, Mar. 4, 2014, *available at* https://krebsonsecurity.com/tag/protectmyid/ (last visited July 16, 2018).

50. All of these injuries suffered by the Plaintiffs and Class Members are a direct and proximate result of the CLA data breach and include:

a. disclosure of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their PII and financial, business, banking, and other accounts;

c. costs associated with the detection and prevention of medical identity theft and unauthorized use of their PII;

d. costs associated with time lost addressing and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the CLA data breach, including finding fraudulent filed tax returns, theft of social security payments, fraudulent charges, cancelling credit cards, evaluating the burden and potential benefit of applying for a new social security number, signing up for and purchasing credit monitoring and identity theft and medical identity theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, time spent without access to credit while a new credit card is being issued, and the stress, nuisance, and annoyance of dealing with all issues resulting from the CLA data breach;

e. the imminent and certain impending injury flowing from fraud and identify theft posed by their PII being placed in the hands of third parties;

f. damages to and diminution in value of their Personal Information entrusted to Defendant for the sole purpose of obtaining employment, with the mutual understanding that Defendant would safeguard against theft dissemination, and take

all steps available to prevent access to or misuse of Plaintiffs' and Class Members' data by unauthorized third parties;

i. continued risk to Plaintiffs' and Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect the Personal Information entrusted to them.

CLASS ACTION ALLEGATIONS

A. STATEWIDE CLASSES

51. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert common law claims for negligence (Count I), negligence per se (Count II), as well as statutory claims under state statutes (Count III), on behalf of separate statewide classes for the states of California, Florida, Texas, Maine, New Jersey, and New York, defined as follows:

52. **Statewide [name of State] Class**: All citizens of [name of state] whose PII was compromised by the CLA data breach.

53. Pursuant to Fed. R. Civ. P. 23, Plaintiff seek to represent a class comprised of all persons in California, Florida, Texas, Maine, New Jersey, and New York who, within the applicable statute of limitations preceding the filing of this action, had their PII compromised in the CLA data breach.

54. Excluded from the Class are all legal entities, Defendant herein and any person, firm, trust, corporation, or other entity related to or affiliated with any defendant, as well as

any judge, justice or judicial officer presiding over this matter and members of their immediate families and judicial staff.

55. Plaintiff nevertheless reserve the right to divide into subclasses, expand, narrow, or otherwise modify the class definition prior to (or as part of) filing a motion for class certification.

56. The members in the proposed class and subclass are so numerous that individual joinder of all members is impracticable, and the disposition of the claims of all class members in a single action will provide substantial benefits to the parties and Court. Fed. R. Civ. P. 23(a)(1). While the exact number of Class members is unknown to Plaintiffs at this time and will be ascertained through appropriate discovery, Plaintiffs are informed and believe that there are at least 130 members. Members of the Class can be identified from the records maintained by Defendant.

57. There are questions of law and fact common to the class, Fed. R. Civ. P. 23(a)(2), which Plaintiff may seek to litigate on an individual basis pursuant to Fed. R. Civ. P. 23(c)(4), including without limitation, that each putative member of the Class had their PII compromised in the CLA data breach.

58. Plaintiffs' claims are typical of the claims of the other members of the putative Class. All Class members have been and/or continue to be similarly affected by Defendant's wrongful conduct as complained of herein, in violation of law. Plaintiffs have no interests adverse to the Class.

59. Plaintiffs will fairly and adequately protect the Class members' interests and have retained counsel competent and experienced in consumer class action lawsuits and complex litigation.

60. Defendant has acted with respect to the putative Class in a manner generally applicable to each Class member. Common questions of law and fact exist as to all members of the Class and predominate over any questions wholly affecting an individual Class member. There is a well-defined community of interest in the questions of law and fact involved in the action, affecting all members of the Class. The questions of law and fact common to the members of the Class include, *inter alia*:

(a) Whether Defendant owed a duty to Plaintiffs and members of the Classes to take reasonable measures to safeguard their Personal Information;

(b) Whether Defendant failed to adequately safeguard Plaintiffs' and the Classes' Personal Information;

(c) Whether Defendant failed to protect Plaintiffs and the Classes' Personal Information;

(d) Whether Defendant knew or should have known that its Human Resources Department's control of the PII was vulnerable;

(e) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Classes' Personal Information properly;

(f) Whether Defendant violated the consumer protection statutes and data breach notification statutes applicable to Plaintiffs and each of the Classes;

(g) Whether Defendant failed to notify Plaintiffs and members of the Classes about the CLA data breach as soon as practicable and without delay after the breach was discovered;

(h) Whether Defendant acted negligently in failing to safeguard Plaintiffs' and the Classes' Personal Information;

(i) Whether Plaintiffs and the members of the Classes are entitled to actual damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

(j) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

(k) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Classes.

61. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it virtually impossible for Class members to individually redress the wrongs done to them. There will be no difficulty in managing this action as a class action.

62. Defendant has acted on grounds generally applicable to the entire Class with respect to the matters complained of herein, thereby making appropriate the relief sought herein with respect to the members of the Class as a whole.

63. As a result of the foregoing, class treatment is appropriate under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3), and may be appropriate for certification "with respect to particular issues" under Rule 23(c)(4).

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

Negligence

Brought by Statewide Classes

64. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

65. Plaintiffs bring this Claim on behalf of the Statewide Classes under their respective state's law.

66. Defendant required Plaintiffs and Statewide Class Members to entrust with Defendant Personal Information as a condition of employment.

67. Defendant, therefore, was entrusted with a massive amount of personally identifiable information belonging to individuals.

68. Defendant collected and stored this data and knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiffs and Statewide Class Members.

69. Defendant owed, undertook, and/or assumed duties of care to use reasonable means to secure and safeguard this Personal Information and to prevent disclosure of the information. Defendant's duties include, among others, a responsibility to implement reasonable technical, administrative, and physical security measures that would permit them to detect, respond to, remedy, and promptly notify affected individuals of security breaches in a reasonably expeditious period of time as well as a duty to maintain PII in a secure fashion.

70. Defendant's duties arise from the common law, state statutes cited in this Complaint. Defendant breached its duties of care by failing to secure and safeguard the Personal Information of Plaintiffs and the Classes. Defendant negligently maintained systems that were vulnerable to a security breach, and knew or should have known of these vulnerabilities.

71. Defendant acted with wanton disregard for the security of Plaintiffs' and Statewide Class Members' Personal Information.

72. A "special relationship" exists between Defendant and the Plaintiffs and Statewide Class Members. Defendant entered into a "special relationship" with the Plaintiffs and Class Members whose Personal Information was requested, collected, and received by Defendant as a condition of employment and because Defendant CLA employed the Plaintiffs and Class Members.

73. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Statewide Class Members, Plaintiffs and Statewide Class Members would not have been injured.

74. The injury and harm suffered by Plaintiffs and Statewide Class Members, was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Statewide Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

75. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and the Statewide Class Members, have suffered injury because, among other things, their Personal Information has been exposed, imminently subjecting each member of the Classes to identity theft, credit and bank fraud, social security fraud, tax fraud, medical identity fraud, and other varieties of identity fraud.

76. Plaintiffs and the Classes have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Classes have suffered, and/or face an

imminent risk of suffering, the theft of Personal Information; costs associated with prevention, detection, and mitigation of identity theft, medical identity theft, and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of, or preventing, fraud in any of its forms, and damages from the unconsented exposure of Personal Information due to this breach.

SECOND CLAIM FOR RELIEF

Negligence Per Se

Brought by Statewide Classes

77. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

78. Pursuant to state laws in the following states, Defendant operating in the states set forth below had a duty to those respective states' Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Personal Information:

a) California: Cal. Civ. Code § 1798.81.5 b.; Cal. Civ. Code § 1798.82;

b) Florida: Fla. Stat. § 501.171(2);

c) N.Y. Gen Bus. Law § 899-aa(2);

d) N.J. Stat. § 56:8-163;

e) Texas Bus. and Comm. Code § 521.053;

f) Maine Comm. and Trade Code §1348;

79. Defendant breached its duties to Plaintiffs and Statewide Class Members under the above-referenced state laws requiring reasonable data security. Defendant breached its duties by failing to provide fair, reasonable, or adequate Information Technology systems and data security practices sufficient to safeguard Plaintiffs' and Class Members' Personal Information.

80. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

81. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiffs and Statewide Class Members, Plaintiffs and Class Members would not have suffered injury as described herein.

82. The injury and harm suffered by Plaintiffs and Statewide Class Members, was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that its duties were not being fulfilled, and that Defendant's breach of duty was likely to cause Plaintiffs and Statewide Class Members to experience the foreseeable harms associated with the loss and/or exposure of Plaintiffs' and Class Members' Personal Information.

83. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF

Violation of State Consumer Protection Laws
Brought by Statewide Classes as Set Forth Below

California

California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq*.

(Brought by California Class Against Defendant)

84. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

85. Plaintiffs bring this claim against Defendant on behalf of California Class Members.

86. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code section 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

87. Defendant is a business that owns, maintain, and license personal information, within the meaning of 1798.81.5, about Plaintiffs and California Class Members.

88. Defendant is not "a provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act," and violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiffs' and California Class Members' Personal Information.

89. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code § 1798.81.5, Plaintiffs and Class Members suffered damages, as described above.

90. Defendant engaged in unfair acts and practices by failing to disclose the CLA data breach to California Class Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. These unfair acts and practices were immoral,

unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members.

91. Defendant engaged in unfair acts and practices by failing to take proper action following the CLA data breach to enact adequate privacy and security measures and protect California Class Members' PII from further unauthorized disclosure, release and data breaches. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members.

92. As a direct and proximate result of Defendant's acts of unfair and unlawful practices and acts, the Plaintiffs were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

93. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard California Class Members' PII and that the risk of a data breach was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Class.

94. California Class Members seek relief under California Business and Professions Code § 17200, *et seq*., including, but not limited to, monetary damages, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civil Pro. §1021.5), and injunctive or other equitable relief.

95. Plaintiffs and California Class Members seek relief under Cal. Civ. Code §1798.84, including, but not limited to, actual damages and injunctive relief.

New York

N.Y. Gen Bus. Law § 899-aa(2)

(Brought by New York Class Against Defendant)

96. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the CLA data breach to New York Class Members in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen Bus. Law § 899-aa(2);

97. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the CLA data breach to enact adequate privacy and security measures and protect New York Class Members' PII from further unauthorized disclosure, release, data breaches, and theft.

98. Defendant systematically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiffs and members of the New York Class.

99. As a direct and proximate result of Defendant's deceptive trade practices, New York Class Members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII, and the loss of the benefit of their respective bargains.

100. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

101. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard New York Class Members' PII and that risk of a data breach or cyber attack was highly likely. Defendant's actions in engaging in the

above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New York Class.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and all Class Members, request the Court to enter judgment against Defendant as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Classes as requested herein, appointing the undersigned interim co-lead counsel as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein.

B. Injunctive relief, and other equitable relief as is necessary to protect the interests of the Class, including an order (i) prohibiting Defendant from engaging in the unlawful and wrongful acts described herein; (ii) requiring Defendant to protect all data collected or received in the regular course of business in accordance with state and local laws, and industry standards and best practices; (iii) requiring Defendant to design, maintain, and test its Information Technology systems to ensure that Personal Information in its possession is adequately secured and protected; (iv) requiring Defendant to disclose future data breaches in a timely and accurate manner; (v) requiring Defendant to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or system deficiencies detected by these audits; (vi) requiring Defendant to audit, test, and train staff security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner; (vii)

requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; (viii) requiring Defendant to encrypt all PII stored in its databases; (x) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner Personal Information no longer necessary for the provision of Defendant's services; (xi) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members; (xii) establishing a fund that would cover the costs to Class Members associated with freezing and unfreezing their credit with the three major credit reporting bureaus; and (xiv) requiring Defendant to educate all Class Members regarding the threats they face as a result of the loss of their PII, and to provide Class Members with steps they may take to protect themselves, as well as any other relief that the Court deems appropriate under the facts of this case.

C. In addition, Plaintiffs request actual damages, punitive damages, statutory damages, exemplary damages, equitable relief, attorneys' fees, statutory costs, and such further relief as is just and proper. Plaintiffs seek attorneys' fees under applicable state and federal law.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Dated: November 16, 2018

DEREK SMITH LAW GROUP, PLLC

/s/ Abe Melamed

ABRAHAM Z. MELAMED
Abe@dereksmithlaw.com
1 Pennsylvania Plaza, suite 4905
New York, New York 10119
Phone: (212) 587-0760